THE WHITE HOUSE
Office of the Press Secretary

For Immediate Release December 1, 2010

FACT SHEET: U.S. Government Mitigation Efforts in Light of the Recent Unlawful Disclosure of Classified Information

As part of an integrated federal government approach to respond to the unlawful and irresponsible disclosure of classified information by Wikileaks, the National Security Staff has been coordinating an interagency effort to examine the policies and practices surrounding the handling of classified information, and to put in place safeguards to prevent such a compromise from happening again.

The 9/11 attacks and their aftermath revealed gaps in intra-governmental information sharing. During the past decade, departments and agencies have tried to eliminate those gaps, resulting in considerable improvement in information-sharing. At the same time, federal policies underscore the importance of the existing prohibitions, restrictions, and requirements regarding the safeguarding of classified information. Our national security requires that sensitive information be maintained in confidence to protect our citizens, our democratic institutions, our homeland and our partners. Protecting information critical to our nation's security is the responsibility of each individual and agency granted access to classified information.

NATIONAL SECURITY STAFF INITIATIVES

On December 1, 2010, the National Security Advisor named Russell Travers to serve as the National Security Staff's Senior Advisor for Information Access and Security Policy. Travers will lead a comprehensive effort to identify and develop the structural reforms needed in light of the Wikileaks breach. His responsibilities will include:

- Advising the National Security Staff on corrective actions, mitigation measures, and policy recommendations related to the breach.
- Facilitating interagency discussions and developing options for Deputies, Principals, and the President regarding technological and/or policy changes to limit the likelihood of such a leak reoccurring.

Additionally, the President's Intelligence Advisory Board (PIAB) will take an independent look at the means by which the Executive Branch as a whole shares and protects classified information. While the PIAB's traditional mandate is the examination of intelligence issues, the members' requisite security clearances, deep understanding of the wider United States Government national security mission and appreciation of the scope and complexity of classified government computer networks, make it particularly well-suited to immediately undertake this U.S. Government-wide review. As a part of this undertaking, the PIAB will:

- Work with departments and agencies across the government to ensure they gain a comprehensive appreciation of all relevant challenges and requirements necessary to safeguard classified information and networks.
- Examine the current posture of the whole of government with regard to leaks of classified information.

- Examine the balance between the need to share information and the need to protect information.
- Review the degree to which the government is organized to achieve information handling goals, consistent with our interests in security, information sharing, and transparency.

These efforts by the NSS and the PIAB will complement actions being taken across the Federal Government. The Office of Management and Budget (OMB) has directed each department or agency that handles classified information establish a security assessment team consisting of counterintelligence, security, and information assurance experts to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. The OMB has directed that each review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure that users do not have broader access than is necessary to do their jobs effectively, as well as implementation of restrictions on usage of, and removable media capabilities from, classified government computer networks. The OMB, the Information Security Oversight Office, and the Office of the Director of National Intelligence will stand up processes to evaluate, and to assist agencies in their review of security practices with respect to the protection of classified information.

Prior to the issuance of this OMB Directive, several agencies had proactively initiated measures to further safeguard classified information and networks. The following are examples of the numerous mitigation efforts underway across the interagency.

DEPARTMENT OF STATE INITIATIVES

The Secretary of State has commissioned a review of State Department security procedures. The Under Secretary for Management has assembled a team of senior management professionals in all related areas to conduct a thorough review of current policies and procedures to ensure that they are fully abreast of the challenges faced. Their efforts will be coordinated with the Bureau of Intelligence and Research to ensure that a measures taken strike the correct balance between the critical need to protect classified information and the equally compelling requirement to ensure that it is shared with those who need it in their work to advance our national security.

This review has already reaffirmed the Department's policy of deploying "thin client" computer units without removable media options and limiting the ability to download material from classified terminals to only approved and controlled circumstances.

The Department will also deploy an automated tool that will continuously monitor the classified network to detect anomalies that would not be readily apparent. This capability will be backed up by a professional staff who will promptly analyze these anomalies to ensure that they do not represent threats to the system.

The mandatory annual training and recertification requirement that all employees must satisfy is being reviewed to see if additional material needs to be added to bolster this on-going effort.

In the interim, the Department has suspended access to the Net Centric Diplomacy (NCD) database of diplomatic reporting , and its classified "ClassNet" web sites and SharePoint sites previously

accessible through the Secret Internet Protocol Router Network (SIPRNet), while retaining access via the Joint Worldwide Intelligence Communications System..

DEPARTMENT OF DEFENSE (DoD) INITIATIVES

On August 12, 2010, Defense Secretary Robert Gates commissioned two reviews to determine what policy, procedural and/or technological shortfalls contributed to the unauthorized disclosure to the Wikileaks website. He specifically directed an assessment to determine if the DoD had appropriately balanced restrictions associated with information security and the need to provide our front-line personnel with the information needed to accomplish their assigned missions.

As a result of these two reviews, a number of findings and recommendations are in the process of being assessed and implemented, including the following:

- Disabling and controlling use of removable storage media on DoD classified networks to prevent download from classified networks.
- Developing procedures to monitor and detect suspicious, unusual or anomalous user behavior (similar to procedures now being implemented by credit card companies to detect and monitor fraud).
- Conducting security oversight inspections in all Combatant Commands.
- Undertaking vulnerability assessments of DoD networks.
- Improving awareness and compliance with information protection procedures. Specific examples being undertaken at the Combatant Command level include:
- Increased "insider threat" training focusing on awareness of associated activity.
- Multi-discipline training between traditional security, law enforcement and information assurance at all echelons.
- The establishment of "Insider Threat Working Groups" to address the Wikileaks incident and prevent reoccurrence.
- Component-determined restricted access to the Wikileaks site to prevent further dissemination or downloading of classified information to unclassified DoD networks.
- Restating of policy to all personnel regarding restrictions on downloading to government systems and cautionary advice regarding personal IT systems.

Individual DoD components are taking additional action as relevant and appropriate, ranging from random physical inspections to enabling new security features on networks. Leadership reinforcement of workforce responsibilities and new initiatives to safeguard information are key components of DoD's mitigation efforts. Department-wide, the Pentagon is accelerating its publication of policy issuances related to the information security program as well as focusing increased attention on detecting potential insider threats.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI) INITIATIVES

The ODNI is working as part of the integrated whole of government approach to assist agencies in their review of security practices.

In coordination with the larger OMB effort, ODNI is developing recommendations to enhance security within the Intelligence Community (IC), to include:

- Insider Threat Assessment Inspections: Departments and Agencies will establish inspection teams, with assistance provided by ODNI/ONCIX, consisting of Counterintelligence (CI), Security, and Information Assurance (IA) experts to identify removable media policies and their implementation.
- Enhanced Automated, On-Line Audit Capability: Systems will monitor user activity on all IC classified computer systems to detect unusual behavior. Additionally, a fully staffed analytic capability will put a human eye on the suspect activity.
- Removable Media Policies Review: Department and Agencies will review current policies and procedures to reduce risk posed by removable media within each organization.
- Policy Compliance Action Plan: Departments and Agencies will assess the level of compliance with existing CI, Security, and IA policies to identify discrepancies and will establish a plan to track and report improvements.
- Information Assurance Training: Departments and Agencies will conduct mandatory regular trainings for all employees on the handling of classified information.
- Review Secure Device Settings: Departments and Agencies will mandate a compliance review of secure system configuration settings.

###
